WHAT IS CLAIMED IS:

1. A public key validation agent (PKVA) comprising:

an off-line registration authority for issuing a first unsigned public key validation certificate (unsigned PKVC) off-line to a subject that binds a public key of the subject to a first public key serial number (PKVN), the registration authority maintaining a certificate database of unsigned PKVCs in which it stores the first unsigned PKVC; and

an on-line credentials server for issuing a disposable public key validation certificate (disposable PKVC) on-line to the subject, the disposable PKVC binds the public key of the subject from the first unsigned PKVC to the first PKVN from the first unsigned PKVC, wherein the credentials server maintains a table that contains entries corresponding to valid unsigned PKVCs stored in the certificate database.

2. The PKVA of claim 1 wherein the first PKVN is different than all previous PKVNs generated by the registration authority.

3. The PKVA of claim 1 wherein the credentials server is responsive to a revocation request from the subject to invalidate the first unsigned PKVC entry in the table of the credential server.

4. The PKVA of claim 3 wherein the registration authority generates a public key revocation code (PKRC) to be used by the subject in its revocation request.

5. The PKVA of claim 4 wherein the registration authority sends the PKRC to the subject over a secure channel that provides data confidentiality.

6. The PKVA of claim 1 wherein the disposable PKVC includes an expiration date/time.

7. The PKVA of claim 6 wherein a validity period from when the credentials server issues the disposable PKVC to the expiration date/time is sufficiently short such that the disposable PKVC does not need to be subject to revocation.

8. The PKVA of claim 6 wherein the disposable PKVC is not subject to revocation.

9. The PKVA of claim 1 wherein the table maintained by the credentials server is a hash table containing cryptographic hashes of valid unsigned PKVCs stored in the certificate database and including a cryptographic hash of the first unsigned PKVC.

10. The PKVA of claim 1 wherein the credential server issues the disposable PKVC in response to a message from the subject containing the issued first unsigned certificate.

11. The PKVA of claim 9 wherein the credentials server computes the cryptographic hash of the first unsigned PKVC with a collision-resistant hash function.

12. The PKVC of claim 11 wherein the collision-resistant hash function is a SHA-1 hash function.

13. The PKVC of claim 11 wherein the collision-resistant hash function is a MD5 hash function.

14. The PKVC of claim 1 wherein the disposable PKVC permits the subject to present the disposable PKVC to a verifier for authentication and for

demonstrating that the subject has knowledge of a private key corresponding to the public key in the disposable PKVC.

5